Alexander Vollmar[1]/Gudrun Görlitz[2]/Kevin Kober[3]

IT-System zur Echtzeitverfolgung von mit GPS-Trackern ausgestatteten Fahrrädern bei Diebstahl unter Berücksichtigung der rechtlichen Rahmenbedingungen

1. Einführung

Im FindMyBike-Projekt wurde in einem interdisziplinären, rechtlich-verwaltungswissenschaftlichen und informationstechnischen Ansatz in Zusammenarbeit mit dem in Berlin ansässigen Unternehmen Noa Technologies GmbH und dem Landeskriminalamt Berlin ein modulares Softwaresystem entwickelt, welches das Auffinden gestohlener Fahrräder mit Hilfe von Positionsbestimmung mittels GPS erleichtert.

Das zu entwickelnde Softwaresystem – im Folgenden *FindMyBike-System* genannt – soll dazu dienen Fahrrad-Live-Positionsdaten von unterschiedlichen Flottenbetreibern bzw. GPS-Trackingservice-Providern[4] über eine standardisierte Schnittstelle datenschutz- und rechtskonform an die Polizei zu übertragen.

Der Einsatz dieses Systems erfordert Änderungen am bisherigen polizeilichen Workflow bei Anzeige und Verfolgung von Fahrraddiebstählen. Bereits heute kann die Erstellung einer Anzeige nach einem Fahrraddiebstahl über die Internet-Wache der Polizei Berlin erfolgen. Mit der Einführung des *FindMyBike-Systems* muss das entsprechende Internet-Formular um neue Felder erweitert werden. Diese Erweiterung umfasst insbesondere die Möglichkeit einer rechtsverbindlichen Freigabe des Gebrauchs der Live-Positionsdaten des gestohlenen Fahrrades.

---

1 Alexander Vollmar war in dem Projekt FindMyBike Wissenschaftlicher Mitarbeiter für die Forschungsfragen aus dem Bereich Informatik.

2 Prof. Dr. Gudrun Görlitz hat das Projekt FindMyBike für den Bereich Informatik geleitet.

3 Kevin Kober war in dem Projekt FindMyBike studentische Hilfskraft für den Bereich Informatik.

4 Im weiteren Verlauf wird der Begriff "Trackingservice-Anbieter" zusammenfassend für alle Flottenbetreiber und GPS-Trackingservice-Provider verwendet.

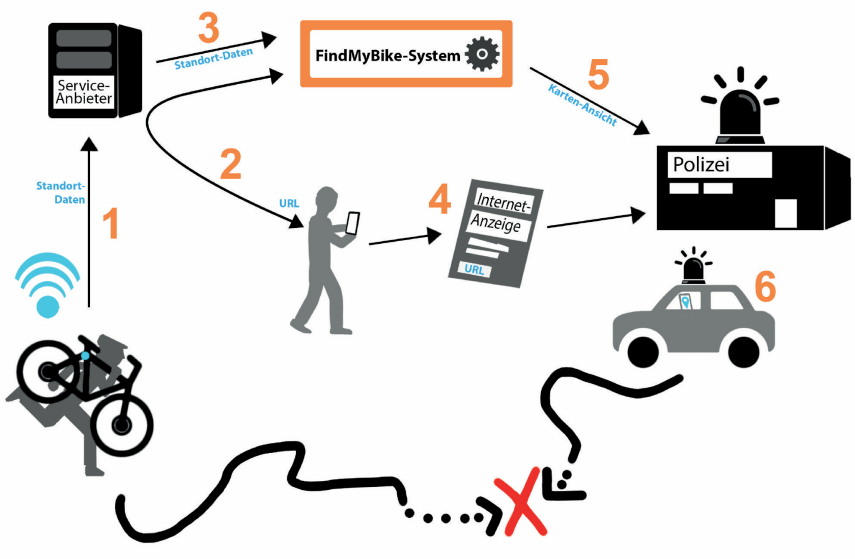

Abbildung 1: Schematische Darstellung der Anzeige und der Verfolgung von Fahrraddiebstählen mit Unterstützung von GPS-Daten (Grafik: Mark Gebler, Alexander Vollmar)

In Abbildung 1 ist die zukünftige Vorgehensweise bei Anzeige und Verfolgung eines Fahrraddiebstahles schematisch dargestellt: Nachdem ein mit einem GPS-Tracker ausgestattetes Fahrrad gestohlen wurde (‚1' in Abbildung 1), bemerkt der*die Besitzer*in den Diebstahl und fordert beim jeweiligen Trackingservice-Anbieter eine URL an (2). Diese URL wird durch das *FindMyBike-System* generiert und vom Trackingservice-Anbieter mit dem Fahrrad verknüpft. Unmittelbar nach dem Abrufen der URL beginnt der Anbieter die Positionsdaten des Fahrrades (mit der URL als ID) an das *FindMyBike-System* zu übermitteln (3). Die bestohlene Person erstellt daraufhin eine Anzeige über die Internet-Wache der Polizei (4) und fügt die vorher abgefragte URL in ein dafür vorgegebenes Feld des Internet-Formulars ein. Die Polizei kann mit Hilfe der URL das *FindMyBike-System* aufrufen und hat damit Zugriff auf eine Kartenansicht, auf der die jeweils letzte bekannte Position des Fahrrades dargestellt wird (5). Mit Hilfe der Anwendung führt die Polizei die Suche nach dem Fahrrad durch und findet im Idealfall sowohl das gestohlene Fahrrad als auch den Dieb (6).

2. Systembeschreibung

Die Hauptaufgabe des *FindMyBike-Systems* besteht im Bereitstellen einer standardisierten Schnittstelle für die Übertragung von Live-Positionsdaten von gestohlenen Fahrrädern von Trackingservice-Anbietern zur Polizei. Diese Schnittstelle soll sämtlichen Anbietern zur Verfügung stehen und die datenschutz- und rechtskonforme Übertragung von Live-Positionsdaten an die Polizei ermöglichen.

2.1 Ablauf der Datenverarbeitung

Die Verarbeitung der Live-Positionsdaten im Gesamtsystem wird von drei unterschiedlichen Akteuren*innen durchgeführt: dem jeweiligen Trackingservice-Anbieter, dem zentralen *FindMyBike-System* sowie der Polizei (siehe Abbildung 2).

Um das System nutzen zu können, muss ein mit einem GPS-Tracker ausgestattetes Fahrrad bei einem Trackingservice-Anbieter angemeldet sein und kontinuierlich seine Positionsdaten an diesen Provider übermitteln. Nachdem ein solches Fahrrad gestohlen und der Diebstahl bemerkt wurde, benötigt die oder der Bestohlene eine URL, die beim *FindMyBike-System* abgerufen werden kann. Dieses Abrufen der URL sollte innerhalb der App des Trackingservice-Anbieters geschehen können, z.B. durch das Drücken eines hierfür vorgesehenen Buttons. Hierdurch wird beim *FindMyBike-System* eine URL angefragt, generiert und an die App weitergeben. Die URL verweist auf eine fahrradspezifische Kartenansicht des *FindMyBike-Systems* und wird zusammen mit dem zugehörigen Zeitstempel in einer Datenbank abgespeichert.

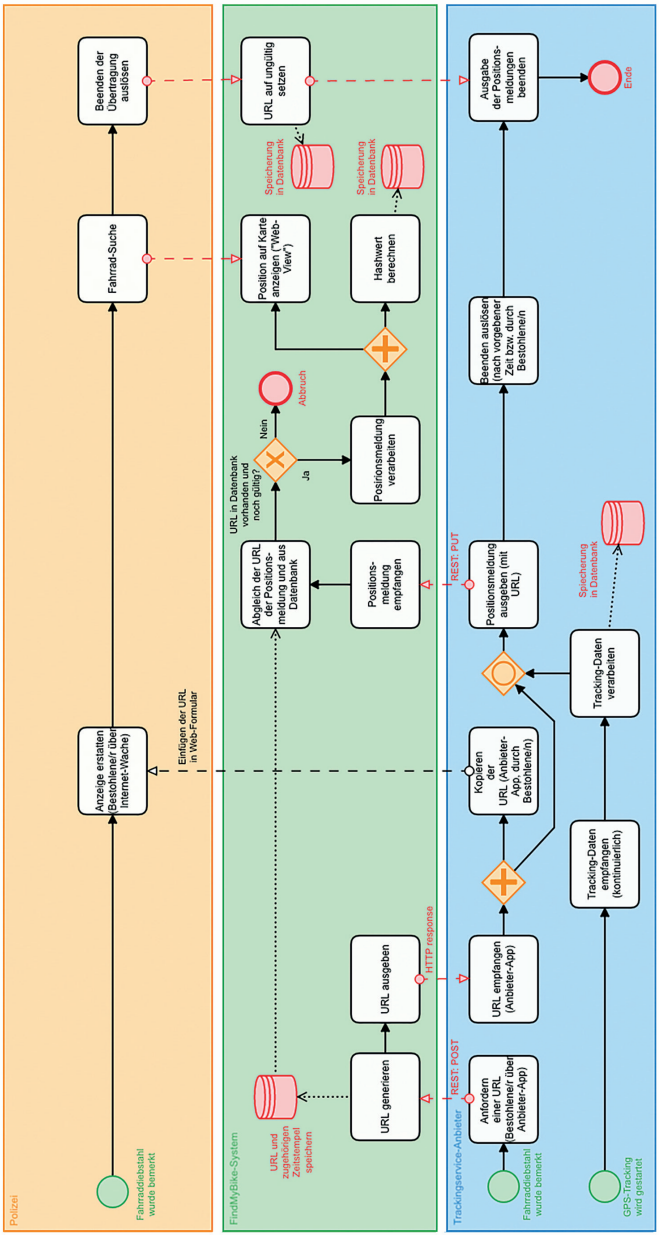

Abbildung 2: FindMyBike-System: Verarbeitung von Positionsdaten (nahezu) in Echtzeit (Grafik: Alexander Vollmar)

Nach dem Abrufen der URL kann mit deren Hilfe eine Diebstahlanzeige über das Internet-Formular der Internet-Wache der Polizei erstattet werden. Die URL wird beim Erstellen der Anzeige in ein eigens dafür vorgesehenes Feld des Webformulars eingefügt.

Sobald die URL vom Trackingservice-Anbieter empfangen wurde, beginnt dieser die Positionsdaten des gestohlenen Fahrrades an das *FindMyBike-System* zu übertragen. Hierbei werden Push-Nachrichten an die oben generierte URL und somit an das *FindMyBike-System* gesendet. Dieses nimmt die Nachrichten mit den Positionsdaten entgegen und fragt in der Datenbank ab, ob die URL existiert und wann sie erstellt wurde. Die URL ist nur innerhalb eines aus rechtlichen Überlegungen festgelegten maximalen Zeitraums gültig. Nach dem Ablauf dieses Zeitraums lehnt es das System ab, Nachrichten mit der jeweiligen URL zu verarbeiten. Falls die URL jedoch in der Datenbank vorhanden und noch gültig ist, wird die Nachricht verarbeitet. Hierbei wird zum einen ein Hashwert über die gesamte Nachricht berechnet und in einer Datenbank abgelegt, zum anderen wird die Position, die aus der Nachricht extrahiert wurde, der URL zugeordnet, so dass dieser bei Aufruf der URL in einer von einem weiteren Service erzeugten Web-View dargestellt werden kann. Der hierbei generierte Hashwert wird später für das nachträgliche Abrufen von Live-Positionsdaten benötigt (siehe 3.3).

Nachdem die Anzeige empfangen wurde, kann die Polizei unter Verwendung der übermittelten URL eine Web-View des *FindMyBike-Systems* öffnen, welche eine Kartenansicht beinhaltet. Auf dieser Karte wird die jeweils letzte bekannte Position des gestohlenen Fahrrades angezeigt. Falls die Position des Gerätes, auf dem das *FindMyBike-System* genutzt wird, und damit auch die Position der Person, die das *FindMyBike-System* gerade verwendet, mit Hilfe der W3C Geolocation API[5] bestimmt werden kann, wird auch dieser auf der Karte visualisiert. Die Angabe der jeweiligen eigenen Position ist insbesondere bei der Suche nach einem Fahrrad im Gelände hilfreich.

2.2 Der Aufbau des FindMyBike-Systems

Das *FindMyBike-System* besteht aus zahlreichen Softwaremodulen, welche die verschiedenen Services realisieren (siehe Abbildung 3). Zentrales Element des Systems ist die Message Broker-Software RabbitMQ, eine nachrichtenorientier-

5 Die Spezifikation der W3C Geolocation API findet sich unter https://www.w3.org/TR/geolocation-API

te Middleware, über die ein großer Teil der internen Kommunikation abgewickelt und eine Parallelisierung von Prozessen umgesetzt wird.

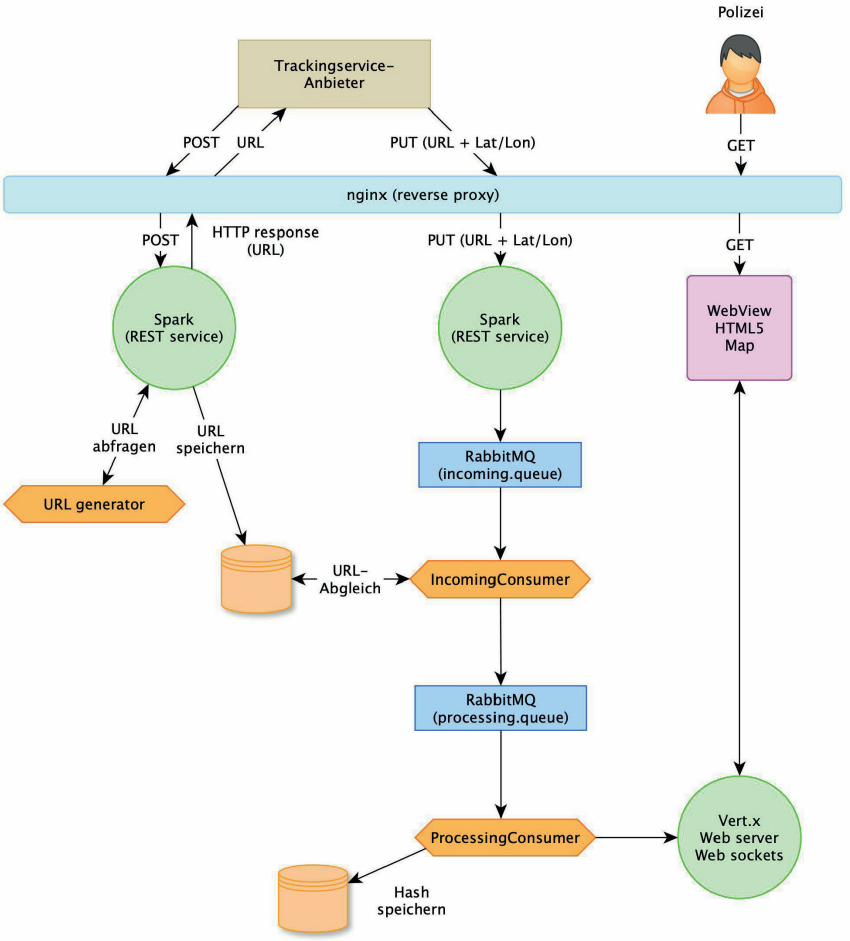

Abbildung 3: Die Zusammenarbeit der verschiedenen Komponenten des FindMyBike-Systems (Grafik: Alexander Vollmar)

Durch das Konzept der Microservice-Architektur ist eine unabhängige Programmierung der verschiedenen Komponenten möglich gewesen. Darüber hi-

naus unterstützt dieser Architekturstil eine agile Entwicklung und ermöglicht insbesondere eine einfache Wartbarkeit eines Systems (und somit die unabhängige Änderbarkeit, Erweiterbarkeit und Ersetzbarkeit der einzelnen Microservices[6]). So kann das Gesamtsystem leicht horizontal skaliert werden, indem die Services auf verschiedene Hostsysteme verteilt und ausgeführt werden. Hierdurch bleibt das System flexibel und es ist sichergestellt, dass es auch bei einer umfangreicheren Nutzung durch eine Vielzahl von Trackingservice-Anbietern, bei einer großen Anzahl an gestohlenen Fahrrädern bzw. bei sehr häufigem Abrufen der Fahrradpositionen performant einsetzbar ist.

Die Kommunikation mit dem *FindMyBike-System* von außen verläuft über einen nginx[7]-Webserver, der als Reverse Proxy fungiert, die HTTP-Requests verarbeitet und diese Anfragen an die verschiedenen Services weiterleitet. Das Web-Application-Framework Spark[8] wird eingesetzt um verschiedene REST[9]-Schnittstellen zur Verfügung zu stellen.

Ein erster Service stellt URLs für die anfragenden Trackingservice-Anbieter bereit. Hierbei wird eine Anfrage nach einer URL zuerst vom Webserver an einen Spark-Service weitergeleitet. Daraufhin erzeugt ein in Kotlin realisierter URL-Generator eine URL und liefert sie an den Spark-Service zurück, der diese wiederum an den Trackingservice-Anbieter weitergibt und zusätzlich in einer dokumentbasierten Datenbank (MongoDB[10]) abspeichert.

Ein weiterer Service dient der Entgegennahme der Positionsdaten. Hierbei beginnt der Trackingservice-Anbieter unmittelbar nach dem oben beschriebenen Empfangen der URL mit der Übertragung der Positionsdaten. Die Positionsnachrichten werden wiederum vom Webserver entgegengenommen und dem Spark-Service übergeben. Dieser Service reicht die Live-Positionsdaten kontinuierlich in eine mit der Message Broker-Software RabbitMQ[11] realisierte Warteschlange weiter, welche die Nachrichten asynchron für die Verarbeitung einem weiteren Kotlin-Programm, dem "incoming consumer" aushändigt. Dieser Consumer gleicht die jeweilige URL mit der Datenbank ab und reicht (falls die URL gültig ist) die Nachricht an eine weitere RabbitMQ-Queue weiter. Von dort wird die Positionsnachricht einem weiteren Consumer ("processing consumer") übergeben, der daraufhin aus der Nachricht einen Hashwert berechnet und diesen in einer weiteren MongoDB-Datenbank speichert. Daneben werden

6 Dowalil 2018, S. 4.
7 nginx unter https://nginx.org
8 http://sparkjava.com
9 REST: Representational State Transfer; ein Programmierparadigma für verteilte Systeme, das häufig für Webservices eingesetzt wird.
10 https://www.mongodb.com
11 https://www.rabbitmq.com

die Positionsdaten aus dieser Message-Queue vom WebServer-Service zum Browser der bzw. des Nutzenden gesendet. Die Übertragung der verschlüsselten Live-Positionsdaten erfolgt dabei über das WebSocket-Protokoll, welches es ermöglicht aktuelle Fahrradpositionen vom Server zum Client zu senden, ohne dass ein kontinuierliches Aktualisieren der Webanwendung durch die Nutzenden erforderlich wäre.

2.3 Sicherheit

2.3.1 Verschlüsselung der Datenübertragung

Zur Verschlüsselung der Datenübertragung zwischen dem Trackingservice-Anbieter, dem *FindMyBike-System* und der Polizei wird das Verschlüsselungsprotokoll "Transport Layer Security" (TLS) eingesetzt. Hierbei wird die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlene TLS-Version 1.2. genutzt. Für die TLS-Version 1.3, die seit dem 21.03.2018 als "proposed standard"[12] gilt, enthalten die Technischen Richtlinien bisher noch keine Einschätzung.[13]

Den Aufbau einer gesicherten Datenverbindung im TLS-Protokoll wird mit Hilfe einer Cipher-Suite, einer standardisierten Sammlung der zu verwendenden kryptographischen Algorithmen für Schlüsseleinigung (und gegebenenfalls auch für die Authentisierung), für die Verschlüsselung der Live-Positionsdaten sowie eine Hashfunktion für die Integritätssicherung der Datenpakete durchgeführt. Das *FindMyBike-System* verwendet eine Cipher-Suite mit Perfect Forward Secrecy (mit der "eine Verbindung auch bei Kenntnis der Langzeit-Schlüssel der Kommunikationspartner nicht nachträglich entschlüsselt werden kann"[14]) und zwar die Cipher-Suite TLS_DHE_RSA_WITH_AES_256_GCM_SHA384. Diese Cipher-Suite ist, wie alle durch das BSI in den Technischen Richtlinien aufgeführten Cipher-Suites,[15] für den Aufbau von gesicherten Datenverbindungen geeignet, wobei der empfohlene Verwendungszeitraum bis über das Jahr 2024 hinaus reicht.

2.3.2 IP-Adress-Bereich

Die URLs mit denen die entsprechenden Kartenansichten des FindMyBike-Systems zur Darstellung derPosition eines gestohlenen Fahrrades aufgerufen werden können, bestehen jeweils im letzten Segment aus einem 64-stelligen

12 Internet Engineering Task Force 2018.
13 Bundesamt für Sicherheit in der Informationstechnik 2018, S. 5.
14 Bundesamt für Sicherheit in der Informationstechnik 2018, S. 7.
15 Bundesamt für Sicherheit in der Informationstechnik 2018, S. 6 ff.

Hexadezimal-String. Eine solche URL ist nur äußerst schwer zu erraten. (Es sind hierbei insgesamt $2^{256} \approx 10^{77}$ verschiedene URLs möglich.) Um einen unberechtigten Zugriff auf die Positionsdaten darüber hinaus auszuschließen, soll die Kartenansicht weiterhin nur aus dem Rechnernetz der Polizei aufrufbar sein. Hierzu wird in der Konfiguration des nginx-Webservers die Möglichkeit des Aufrufs auf Adressen aus dem IP-Bereich der Polizei begrenzt.

3. Die Schnittstellen

Das *FindMyBike-System* benötigt verschiedene Datenschnittstellen für die Kommunikation mit den Trackingservice-Anbietern auf der einen Seite und der Polizei auf der anderen Seite. Diese müssen für das Funktionieren des Gesamtsystems von den verschiedenen Kommunikationspartnern implementiert bzw. genutzt werden. Nachfolgend werden diese Schnittstellen als Vorschlag für eine mögliche Standardisierung des Datenaustauschs ausführlicher beschrieben. Allen Schnittstellen ist gemein, dass der Grundsatz der Datenminimierung beachtet wird, d.h. es werden nur solche Daten übertragen, die für den Betrieb des Systems und die Ermittlungsarbeit der Polizei auch wirklich notwendig sind. Auf eine Speicherung von personenbezogenen Daten durch das *FindMyBike-System* kann dabei vollständig verzichtet werden.

3.1 Übertragung von Tracking-Daten an das FindMyBike-System

Um Positionsdaten übertragen zu können, muss der jeweilige Trackingservice-Anbieter über eine erste Schnittstelle eine fallbezogene URL beim *FindMyBike-System* abfragen. Über eine zweite Schnittstelle sendet der Anbieter nahezu in Echtzeit Nachrichten mit den jeweils aktuellen Positionsdaten des gestohlenen Fahrrads an das *FindMyBike-System*.

3.1.1 Schnittstelle zur Abfrage einer URL durch einen Trackingservice-Anbieter beim FindMyBike-System

Für die eindeutige Zuordnung der Anzeige über die Internet-Wache zu den zugehörigen Positionsmeldungen wird eine ID benötigt. Als ID wird eine URL genutzt, die über eine REST-Schnittstelle beim *FindMyBike-System* abgefragt wird. Für das Durchführen dieser Abfrage wird die HTTP-Methode POST

genutzt. Diese Methode wird hierbei eingesetzt, da sie für nicht idempotente[16] Anfragen, bei denen eine neue Ressource unterhalb der jeweils angegebenen Ressource erstellt wird, verwendet werden soll[17].

Der Abruf einer URL könnte z.B. mit curl[18], einem Programm zum Übertragen von Dateien in Rechnernetzen, wie folgt durchgeführt werden:

```
curl·-X·POST·-k·https://ip029248.beuth-hochschule.de/bike
```

Der Server liefert als Antwort (im Body der HTTP response) eine in ein JSON[19]-Format gekapselte URL. Diese URL muss beim Erstatten einer Anzeige über die Internet-Wache der Polizei in das hierfür vorgesehene Feld eingegeben werden. Nachfolgend ist ein Beispiel für den response body der Antwort des Servers (mit dem zugehörigen HTTP-Statuscode 201, "created") aufgeführt:

```
{
··"url":··"https://[findmybikeserver.de]/bike/77DEED7EE6D42DAB96F0764096CBD0FBA
E4AEFDDFA121FE480F75D9B85851554"
}
```

Die vom *FindMyBike-System* generierte URL setzt sich wie folgt zusammen:

```
https://[findmybikeserver.de]/bike/[ID]
```

Das letzte Segment der URL (oben mit [ID] bezeichnet) besteht aus einem beliebigen 64-stelligen Hexadezimalstring. Falls bei einer Fehlfunktion des Systems die Ausgabe einer URL durch den Spark-Webservice nicht möglich sein sollte, wird eine Antwort mit einem leeren response body und dem HTTP-Statuscode 503 ("service unavailable") zurückgegeben.

Die URL wird zusammen mit dem zugehörigen Zeitstempel (dem Erstellungszeitpunkt der URL) durch das *FindMyBike-System* abgespeichert. Mit Hilfe dieses Zeitstempels kann später ermittelt werden, ob mittels der jeweiligen URL das Abrufen von Positionsdaten zu einem späteren Zeitpunkt noch möglich ist. Hierzu wird im *FindMyBike-System* gemäß rechtlicher Vorgaben eine maximale Gültigkeit für die URLs hinterlegt. Nach Ablauf dieser Frist

16 Idempotenz: Das mehrmalige Ausführen einer Anfrage führt zum gleichen Ergebnis wie eine einzige Ausführung. Die angegebene Methode ist nicht idempotent, d.h. jedes Ausführen führt zu einem neuen Ergebnis, hier dem Generieren einer neuen URL.

17 Richardson/Amundsen/Ruby 2013, S. 37.

18 https://curl.haxx.se

19 JavaScript Object Notation, siehe http://json.org

wird das Abrufen von Positionsdaten für das entsprechende Fahrrad durch das System verweigert.

3.1.2 Schnittstelle zum Versand von Positions-Nachrichten an das FindMyBike-System

Trackingservice-Anbieter, die das *FindMyBike-System* nutzen wollen, müssen Live-Positionsdaten von gestohlenen Fahrrädern mittels Push-Nachrichten an das *FindMyBike-System* übermitteln (auch hier wiederum über die REST-Schnittstelle).

Der Versand der Live-Positionsdaten muss dabei kontinuierlich erfolgen, d.h. es wird, sobald vom Trackingservice-Anbieter eine neue Positionsmeldung des GPS-Trackers eines betroffenen Fahrrads empfangen wurde, eine entsprechende Nachricht mit der letzten Positions-Meldung an das *FindMyBike-System* gesendet. Die Positionsnachrichten umfassen lediglich die folgenden Felder:

Tabelle 1: Positionsnachricht

Feld-Bezeichnung	**Beschreibung**
location	JSON-Objekt mit zwei Feldern für die geographische Länge (*longitude*) und Breite (*latitude*) der Position des Fahrrads
timestamp	Der Zeitpunkt, auf den sich die Positionsmeldung bezieht (Unixzeit)
Accuracy	Genauigkeit des GPS-Geräts (in Metern)[20]

Als Format für die Positionsmeldungen wird wiederum JSON eingesetzt. Nachfolgend ist eine Beispiel-Nachricht dargestellt:

```
{
··"location":·{
·····"longitude":·13.351520729064941,
·····"latitude":·52.539655456542969
},
··"timestamp":·1531927644,
··"accuracy":·14
}
```

20 Die Genauigkeit eines GPS-Trackers beschreibt den Radius in dem sich das Gerät mit einer bestimmten Wahrscheinlichkeit befindet. Diese Wahrscheinlichkeit ist nicht normiert und kann bei verschiedenen Geräten unterschiedlich sein.

Positionsnachrichten mit der oben aufgeführten Struktur können mittels der HTTP-Methode PUT an die REST-Schnittstelle des *FindMyBike-Systems*, d.h. an die oben abgerufene URL (siehe 3.1.1), gesendet werden:

Die Methode PUT wird im REST-Architekturstil zum Anlegen von Ressourcen verwendet und ist idempotent. Wird eine identische Nachricht also mehrmals an den Server gesendet, so wird sie nur beim ersten Mal verarbeitet und sie hinterlässt den Server im jeweils selben Zustand.

Nach dem Empfangen einer Positionsnachricht durch den Trackingservice-Anbieter, wird dem *FindMyBike-System* somit eine neue Nachricht mittels der PUT-Methode übermittelt und damit eine neue Ressource mit den jeweiligen Positionsdaten erstellt. Das System berechnet mittels einer kryptographischen Hashfunktion (aus der SHA-2-Familie, SHA-512/256[21]) aus der Positionsnachricht einen Hashwert. Dieser Hashwert, eine ID (das letzte Segment der URL) sowie der entsprechende Zeitstempel werden in einer Datenbank abgelegt. Die eigentlichen Positionsdaten werden also aus datenschutzrechtlichen Gründen nicht in der Datenbank abgespeichert. Mit Hilfe des Hashwerts kann bei einem erneuten Abrufen der Positionsdaten überprüft werden, ob die zugehörigen Daten beim Anbieter verändert wurden.

Beispiel für das Versenden einer Push-Nachricht an das *FindMyBike-System* mit curl:

```
curl·-H·'Content-Type: ·application/json'·-X ·PUT·-d·'{·"location":·{·"longitude":
·13.351520729064941, ·"latitude":·52.539655456542969·},·"timestamp":·1531927644,
·"accuracy":·14}'·-k https:// [findmybikeserver.de]/bike/77DEED7EE6D42DAB96F07
64096CBD0FBAE4AEFDDFA121FE480F75D9B85851554
```

Der Server liefert, falls er die Nachricht entgegennehmen kann, eine HTTP-Antwort mit einem “ok” im response body und dem HTTP-Statuscode 202 (“accepted”). Falls die Positions-Meldung nicht entgegengenommen werden kann, wird als Antwort ein leerer response body und der HTTP-Statuscode 503 (“service unavailable”) zurückgegeben.

3.2 Darstellung der Positionsdaten auf einer Karte

Mit Hilfe der erstellten URL kann die Polizei auf die jeweils aktuelle Position eines gestohlenen Fahrrades zugreifen. Diese Position wird auf einer Web-View visualisiert (siehe Abbildung 4). Wenn neue Positionsdaten des Fahrrades vor-

21 Siehe hierzu Gueron/Johnson/Walker 2010; eine genaue Beschreibung der Hashfunktionen nach dem SHA-Standard findet sich in *National Institute of Standards and Technology* (2015); Informationen zur Berechnung eines SHA-512/256-Hashs ebenda S. 26.

liegen, wird die Anzeige der Position in dieser Kartenansicht automatisch aktualisiert (also jeweils nachdem eine neue, aktuelle Meldung verarbeitet wurde).

Beim Öffnen der Kartenansicht wird, soweit sich die entsprechende Information im Arbeitsspeicher des FindMyBike-Servers befindet, die letzte Position, die dem System bekannt ist, auf der Karte dargestellt. Diese Information wird allerdings nicht dauerhaft durch das System gespeichert und geht z.B. nach einem Neustart des Servers verloren. Wenn seit dem Start des *FindMyBike-Systems* keine neuen Positionsdaten übermittelt wurden, kann solange kein Position visualisiert werden, bis eine erste Positionsmeldung empfangen wurde. Falls sich das Fahrrad z.B. in einem abgeschirmten Raum befindet, kann eine solche Meldung damit auch ganz ausbleiben.

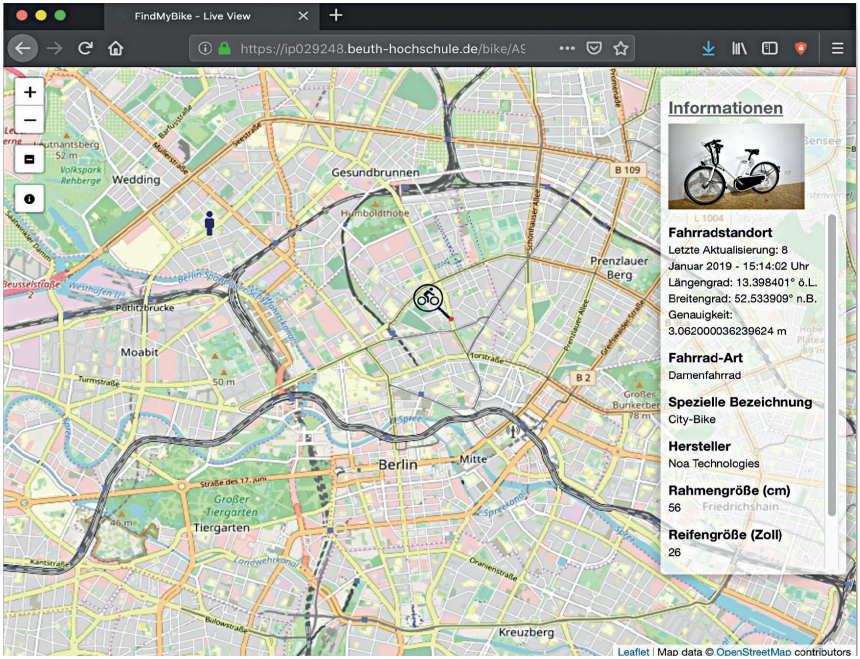

Abbildung 4: Screenshot der FindMyBike-Anwendung: Karteansicht mit Symbolen für das gestohlene Fahrrad und die Position des jeweilig genutzten Gerätes

Der Abruf der Karte kann mittels eines gewöhnlichen Web-Browsers durch Eingabe der URL erfolgen. (Es wird hierbei also die HTTP-Methode GET verwendet.) Auf der Karte kann zusätzlich zur Position des jeweiligen Fahrrades auch die Position des entsprechenden Tablets oder sonstigen mobilen Endgeräts (und somit auch der Standpunkt der Person, welche das *FindMyBike-System* gerade einsetzt) dargestellt werden. Die Kartenansicht wird auf Grundlage von OpenStreetMap[22] bereitgestellt. Die HTML5-basierte Webanwendung verwendet die Bibliothek Leaflet[23] um die Web Map Tiles ("Karten-Kacheln") von OpenStreetMap anzuzeigen.

3.3 Schnittstelle zum rückwirkenden Abruf von Positionsdaten durch die Polizei beim Trackingservice-Anbieter – vermittelt durch das FindMyBike-System

Neben der oben dargestellten Möglichkeit des Empfangens von Positionsdaten nahezu in Echtzeit kann die Polizei, wenn die Positionsdaten für die Beweisführung vor Gericht benötigt werden, rückwirkend beim Trackingservice-Anbieter anfragen (siehe Abbildung 5).

22 https://www.openstreetmap.org
23 https://leafletjs.com

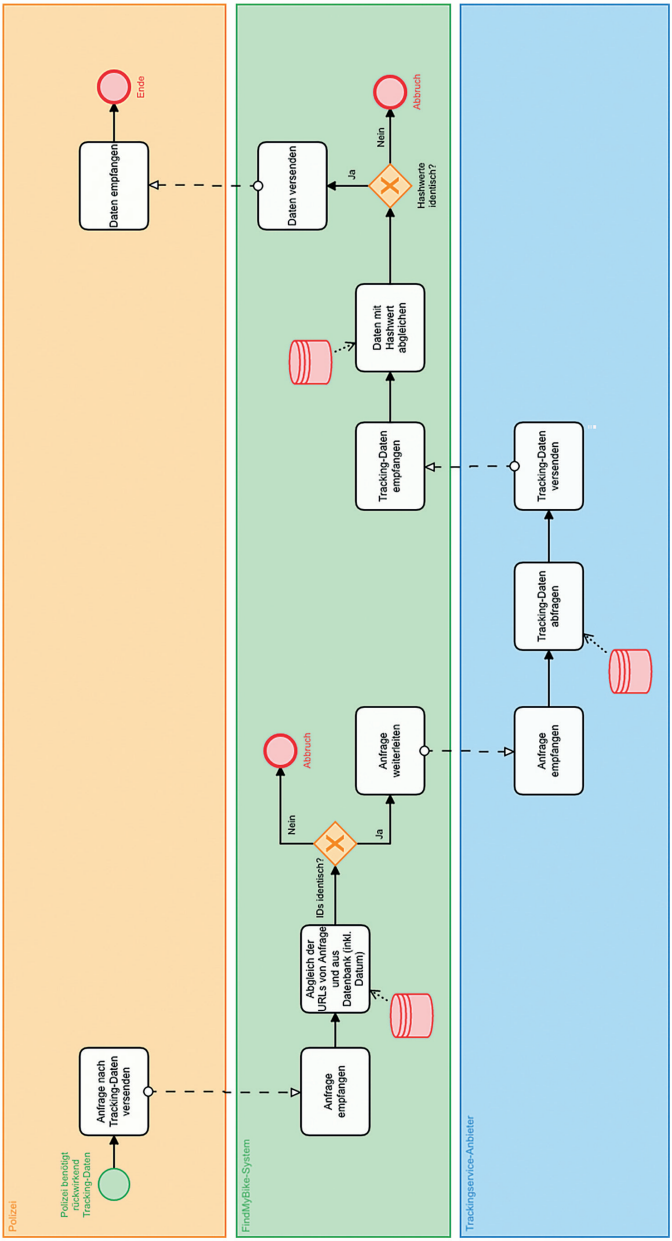

Abbildung 5: FindMyBike-System: Rückwirkender Abruf von Positionsdaten durch die Polizei (Grafik: Alexander Vollmar)

Die Live-Positionsdaten werden durch das *FindMyBike-System* mit den zwischengespeicherten Hashwerten abgeglichen und bei Übereinstimmung in standardisierter Form an die Polizei weitergereicht. Die Abfrage ist frühestens ab dem Zeitpunkt der Erstellung der URL möglich.

Für diesen rückwirkenden Abruf wird eine Nachricht (Aufbau siehe Tabelle 2), welche die URL und den Zeitpunkt, ab dem die Freigabe besteht, beinhaltet, von der Polizei an das *FindMyBike-System* gesendet. Das *FindMyBike-System* gleicht die URL mit der Datenbank ab und leitet, falls diese in der Datenbank vorhanden ist, die Anfrage an den Trackingservice-Anbieter weiter. Der Provider versendet hierauf alle Nachrichten (siehe Tabelle 3) mit den zu dem Fahrrad vorhandenen Positionsdaten – ab dem entsprechenden, angegebenen Zeitpunkt.

Tabelle 2: Anfrage an den Trackingservice-Anbieter

Feld-Bezeichnung	**Beschreibung**
url	wurde beim FindMyBike-System abgefragt (siehe 3.1.1)
timestamp	Zeitpunkt ab dem die Positionsdaten abgerufen werden sollen

Tabelle 3: Beispiel für eine erneut gesendete Positionsmeldung (vom Trackingservice-Anbieter an das FindMyBike-System)

Feld-Bezeichnung	**Beschreibung**
location	JSON-Objekt mit zwei Feldern für die geographische Länge (*longitude*) und Breite (*latitude*) der Position des Fahrrads
timestamp	Der Zeitpunkt, auf den sich die Positionsmeldung bezieht (Unixzeit)
accuracy	Genauigkeit des GPS-Geräts (in Metern)

Die Positionsmeldungen, die erneut gesendet werden, müssen identisch zu den unter 3.1.2 versandten Nachrichten sein. Aus diesen nochmals versendeten Positionsnachrichten werden durch das *FindMyBike-System* wiederum Hashwerte berechnet und mit den entsprechenden, in der Datenbank abgespeicherten Hashwerten abgeglichen. Mit Hilfe der Hashwerte kann gezeigt werden, dass die Positionsdaten zwischen der ersten und der erneuten Übertragung nicht verändert wurden, d.h. die Gleichheit der Datensätze kann somit nachgewiesen

werden[24]. Bei Übereinstimmung der Hashwerte werden alle Positionsnachrichten in einem Arbeitsgang, z.B. als zip-Archiv, an die Polizei weitergeleitet.

3.4 Schnittstelle für die Beendigung der Datenübertragung

Die Übertragung von Positionsdaten vom Trackingservice-Anbieter über das *FindMyBike-System* an die Polizei kann auf verschiedenen Wegen beendet werden (siehe auch Abbildung 2). Zum einen sollte der Serviceanbieter die Übertragung der Live-Positionsdaten automatisch nach einer vorgegebenen Zeit beenden. Diese Zeit sollte aus den rechtlichen Vorgaben abgeleitet werden und prinzipiell verhindern, dass Daten über eine rechtlich abgesicherte Zeitspanne hinaus an die Polizei übertragen werden können. Zum anderen sollte auch die bestohlene Person die Übertragung abbrechen können. Ein einfacher Weg dies zu realisieren ist das Integrieren eines Schalters in die App des jeweiligen Providers, über welchen die Datenübertragung direkt abgebrochen werden kann, z.B. nach dem Auffinden des Fahrrads. Diese beiden Abbruchmöglichkeiten müssen bei Nutzung des FindMyBike-Systems durch den entsprechenden Anbieter implementiert werden.

Weiterhin wird in die Web-View zur Darstellung der Positionsdaten eines gestohlenen Fahrrads bei der Polizei ein Schalter integriert, über den der Wunsch zum Abbruch der Datenübertragung an das *FindMyBike-System* gemeldet und von diesem an den jeweiligen Anbieter weitergeleitet wird. Hiermit wird die Polizei in die Lage versetzt zu jedem beliebigen Zeitpunkt den Prozess abbrechen zu können, z.B. wenn ein Fahrrad wieder aufgefunden oder eine Anzeige zurückgezogen wurde und somit die rechtliche Grundlage für die Datenübertragung nicht mehr besteht.

4. Ausblick

Für den zukünftigen Einsatz des *FindMyBike-Systems* durch die Polizei wäre es über die oben beschriebenen Anpassungen vorteilhaft, wenn die Fahrrad-Diebstahlsanzeige direkt aus der Fahrradpass-App[25] der "Polizeilichen Kriminalprävention der Länder und des Bundes"[26] (oder einer ähnlichen Anwendung)

24 *Heinson* (2015), S. 146ff.

25 Informationen zur Fahrradpass-App finden sich unter https://www.polizei-beratung.de/themen-und-tipps/diebstahl-und-einbruch/diebstahl-von-zweiraedern/fahrradpass-app

26 Das Programm Polizeiliche Kriminalprävention der Länder und des Bundes ist ein Verbund zwischen den Polizeien der Bundesländer, der Bundespolizei, des Bundeskriminalamts und der Deutschen Hochschule der Polizei. Siehe hierzu https://www.polizei-beratung.de

erstattet werden könnte. Diese App sollte zu diesem Zweck so erweitert werden, dass sie alle für eine Anzeige benötigten Daten zum Fahrrad (inklusive Fotos) und seinem*seiner Besitzer*in bereitstellen kann. Hierzu müsste der oben beschriebene Ablauf der Datenverarbeitung des Gesamt-Systems jedoch verändert werden, da die Anzeige direkt in der Fahrradpass-App erstellt werden sollte. Weiterhin könnte die App die für die Anzeige benötigte URL direkt beim *FindMyBike-System* abrufen und an den Trackingservice-Anbieter übermitteln. Die Nutzung der Internet-Wache für die Erstellung der Anzeige könnte damit vollständig entfallen. In einem weiteren Schritt sollte die Fahrradpass-App für die Nutzung durch die verschiedenen Polizeibehörden aller Bundesländer angepasst werden, so dass die Anzeige durch die App (dem Ort des Diebstahls entsprechend) an die zuständige Polizeistelle im jeweiligen Bundesland weitergeleitet wird.

Literatur

Bundesamt für Sicherheit in der Informationstechnik (2018) Technische Richtlinie TR-02102–2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS), (Version 2018–01). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=6, zuletzt besucht am 20.02.2019.

Dowalil, Herbert (2018) Grundlagen des modularen Softwareentwurfs – Der Bau langlebiger Mikro- und Makro-Architekturen wie Microservices und SOA 2.0. München: Carl Hanser Verlag.

Gueron, Shay.; Johnson, Simon; Walker, Jesse (2010) SHA-512/256. International Association for Cryptologic Research. https://eprint.iacr.org/2010/548.pdf; zuletzt besucht am 20.02.2019.

Heinson, Dennis (2015) IT-Forensik. Veröffentlichungen zum Verfahrensrecht 199. Tübingen: Mohr Siebeck.

Internet Engineering Task Force (2018) Protocol Action: 'The Transport Layer Security (TLS) Protocol Version 1.3' to Proposed Standard. https://www.ietf.org/mail-archive/web/ietf-announce/current/msg17592.html, zuletzt besucht am 20.02.2019.

National Institute of Standards and Technology – Information Technology Laboratory (2015) Secure Hash Standard (SHS). Federal Information Processing Standards, FIPS PUB 180–4. Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS. 180-4.pdf, zuletzt besucht am 20.02.2019.

Richardson, Leonard; Amundsen, Mike; Ruby, Sam (2013) RESTful Web APIs – Services for a Changing World. Sebastopol CA.: O'Reilly Media.